APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,450	11/26/2003	Hung-Hsiang Jonathan Chao	CHAO 1-77-1-14 (LCNT/1260	5965

46363 7590 11/20/2007

PATTERSON & SHERIDAN, LLP/
LUCENT TECHNOLOGIES, INC
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER	
KANE, CORDELIA P	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
11/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/723,450	**Applicant(s)** JONATHAN CHAO ET AL.	
	Examiner Cordelia Kane	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,15,18-21,23 and 25-28* is/are rejected.

7)☒ Claim(s) *13,14,16, 17, 22 and 24* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 March 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *3/5/04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to the non-provisional application filed on November 26, 2003. Claims 1 – 28 are pending. Claims 1, 8, 18, 26, 27 and 28 are independent.

Specification

2. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

3. Claim 10 is objected to because of the following informalities: it does not make any sense and appears to be missing important words. Appropriate correction is required.

4. Claims 4 and 5 are objected to because of the following informalities: the formulas in the claims do not define the variables that are used.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 3, 8 – 12, 15, 18 – 21, 23, and 25 – 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Chesla et al's US Publication 2004/0250124 A1.

Referring to claim 1, Chesla teaches:

a. Confirming a DDoS attack at a network location using a plurality of packet attribute values aggregated from said routers (page 23, paragraph 376). Since the routers are between the security appliance and the WAN, the information would have to come from the routers (Figure 1C).

b. Computing an aggregate conditional probability measure for each packet entering said location based on a selected attributes included within said packets (page 14, paragraph 224).

c. Computing an aggregate cumulative distribution function of scores based on said computed aggregate conditional probability function (page 14, paragraph 225).

d. Determining a discarding threshold using said cumulative probability function (page 14, paragraph 225).

e. Sending said discarding threshold to each of the routers (page 20, paragraph 323). Since the filtering would be in the routers then the information computed in the FIS module would have to be passed to the filters/routers, to be able to filter.

7. Referring to claim 3, Chesla teaches granting immunity to packets of a specified sub-type entering said location (page 13, paragraph 199).

8. Referring to claim 8, Chesla teaches:

f. Aggregating victim destination prefix lists and attack statistics associated with incoming packets received from said plurality of routers (page 14, paragraph 224) to confirm a DDoS attack (page 23, paragraph 376). Since each potential victim would have the same prefix since it is on the same customer network, the aggregating of the statistics would also be an aggregation of the victim prefix list.

g. Aggregating packet attribute distribution frequencies for incoming victim related packets received from said plurality of security perimeter routers (page 14, paragraph 224).

h. Generating common scorebooks from said aggregated packet attribute distribution frequencies and nominal traffic profiles (page 14, paragraph 225).

i. Providing to each of the router a common discarding threshold, said discarding threshold defining a condition in which an incoming packet may be discarded (page 20, paragraph 323). Since the filtering would be in the routers then the information computed in the FIS module would have to be passed to the filters/routers, to be able to filter.

9. Referring to claim 9, Chesla teaches comparing measured attribute values with nominal attribute values, and identifying increases in said measured attribute values over said nominal values (page 9, paragraph 137).

10. Referring to claim 10, Chesla teaches determining if said increase for said measured attribute value exceeds respective predetermined thresholds (page 9, paragraph 137).

11. Referring to claim 11, Chesla teaches that attack statistics includes flow counts (page 3, paragraph 33).

12. Referring to claim 12, Chesla teaches receiving packet attribute distribution frequencies including incoming packet attribute information comprising at least TTL (page 4, paragraph 45).

13. Referring to claim 15, Chesla teaches computing a partial score of different attributes and computing a weighted sum of the partial scores to yield a logarithmic function of conditional legitimate probability (page 15, paragraph 236).

14. Referring to claims 18 and 28, Chesla teaches:

j. Sending victim destination prefix list and attack statistics associated with incoming packets to a centralized controller adapted to confirm a victim of DDoS attach (page 20, paragraph 322-323).

k. Sending packet attribute distribution frequencies for incoming victim related packets (page 16, paragraph 243).

l. Receiving from said centralized controller common scorebooks formed by aggregated packet attribute distribution frequencies (page 14, paragraph 225).

m. Sending local cumulative distribution function of scores to said centralized controller (page 13, paragraph 212).

n. Discarding incoming packets based on a commonly distributed discarding threshold defined by said centralized controller (page 23, paragraph 372)

15. Referring to claim 19, Chesla teaches classifying packets as suspicious or non-suspicious (page 17, paragraph 264) based on the destination address of the packet (page 17, paragraph 278).

16. Referring to claim 20, Chesla teaches that attack statistics includes flow counts (page 3, paragraph 33).

17. Referring to claim 21, Chesla teaches receiving packet attribute distribution frequencies including incoming packet attribute information comprising at least TTL (page 4, paragraph 45).

18. Referring to claim 23, Chesla teaches:

o. Determining a predetermined number of packets to monitor (page 16, paragraph 247).

p. For each incoming packet: determining attribute scores and locally aggregating said scores (page 16, paragraph 247).

q. Forming said CDF from said aggregated scores associated with the predetermined number of incoming packets (page 16, paragraph 249).

19. Referring to claim 25, Chesla teaches:

r. Determining whether a score of an incoming packet is less than or equal to said discarding threshold, discarding said incoming packet if said score is less than or equal to said threshold, and forwarding the incoming packet if said score is greater than the threshold (page 11, paragraph 173).

20. Referring to claim 26, Chesla teaches:

s. Means for aggregating a plurality of packet attribute values respectively received from said routers to confirm said attack at said location (page 23, paragraph 376). Since the routers are between the security appliance and the WAN, the information would have to come from the routers (Figure 1C).

t. Means for computing an aggregate conditional probability measure for each packet entering said location based on selected attributes included within said packet from each location (page 14, paragraph 224).

u. Means for computing an aggregate cumulative distribution function (CDF) based on said computed aggregate conditional probability measures (page 14, paragraph 225).

v. Means for determining a drop threshold based on access to said cumulative probability function (page 14, paragraph 225).

w. Means for sending said drop threshold to each of said routers, (page 20, paragraph 323) wherein said routers are adapted to pass through packets that exceed said determined drop threshold to said location (page 20, paragraph 322).

21. Referring to claim 27, Chesla teaches:

x. Means for aggregating, local victim destination prefix lists and attack statistics associated with incoming packets received from a plurality of routers (page 14, paragraph 224) forming a security perimeter in said network to confirm a victim of said DDoS attack (page 23, paragraph 376). Since each potential victim would have the same prefix since it is on the same customer network, the aggregating of the statistics would also be an aggregation of the victim prefix list.

y. Means for aggregating packet attribute distribution frequencies for incoming victim related packets received from said plurality of security perimeter routers (page 14, paragraph 224).

z. Means for generating common scorebooks from said aggregated packet attribute distribution frequencies and nominal traffic profiles (page 14, paragraph 225).

aa. Means for aggregating local cumulative distribution function (CDF) of the local scores derived from said plurality of security perimeter routers (page 13, paragraph 212).

bb. Means for providing, to each of said plurality of security perimeter routers, a common discarding threshold, said discarding threshold defining a condition in which an incoming packet may be discarded at said security perimeter (page 20, paragraph 323). Since the filtering would be in the routers then the information computed in the FIS module would have to be passed to the filters/routers, to be able to filter.

22. Claims 1 – 7 and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Lau et al's US Publication 2004/0062199 A1.

23. The applied reference has a common inventor and assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it

constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

24. Referring to claim 1, Lau teaches:

cc. Confirming a DDoS attack at a network location using a plurality of packet attribute values aggregated from said routers (page 1, paragraphs 4 and 14).

dd. Computing an aggregate conditional probability measure for each packet entering said location based on a selected attributes included within said packets (page 3, paragraph 41).

ee. Computing an aggregate cumulative distribution function of scores based on said computed aggregate conditional probability function (page 3, paragraph 41).

ff. Determining a discarding threshold using said cumulative probability function (page 2, paragraph 31).

gg. Sending said discarding threshold to each of the routers (page 2, paragraph 16). The router and network processor may be the same unit and therefore the threshold is sent to the router as soon as it is calculated.

25. Referring to claim 2, Lau teaches updating an individual marginal probability mass function and a join probability mass function (page 3, paragraph 41).

26. Referring to claim 3, Lau teaches granting immunity to packets of a specified sub-type entering said location (page 2, paragraph 31).

27. Referring to claim 4, Lau teaches the equation: CP (p) = n /m *JP n/ JP m (A = a p , B = b p , C = c p ,) /(A = a p , B = b p , C = c p ,) (page 2, equation 1).

28. Referring to claim 5, Lau teaches the equation: CP (p) = n/m * Pn(A= ap)/Pm(A=ap)* Pn(B= bp)/Pm(B=bp)* Pn(C= cp)/Pm(C=cp) (page 2, equation 2).

29. Referring to claim 6, Lau teaches that the discarding threshold is calculated using a load shedding algorithm, combined with an inverse lookup on the aggregate CDF of scores (pages 4-6, paragraph 61).

30. Referring to claim 7, Lau teaches that said joint and marginal probability functions are maintained using iceberg-style histograms (page 4, paragraph 46).

31. Referring to claim 26, Lau teaches all the limitations that are equivalent to claim 1, and passing through packets that exceed said determined drop threshold to said location (page 1, paragraph 7).

Allowable Subject Matter

32. Claims 13, 14, 16, 17, and 22, and 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cordelia Kane whose telephone number is 571-272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CPK

Cordelia Kane
Patent Examiner
Art Unit 2132

Gilbert

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100